|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing | |  |
|  | Interim guidance  21 May 2020 |  |  |
|  |  |  |  |

# Background

This interim guidance is intended to inform public health programmes and governments that are considering whether to develop or implement digital proximity tracking technologies for COVID-19 contact tracing. This document includes (a) ethical principles; (b) technical considerations and requirements that are consistent with such principles; and (c) processes that could help achieve equitable and appropriate use of such technologies, including through the implementation of suggested technical considerations and requirements.

Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission. When systematically applied, contact tracing will break the chains of transmission of an infectious disease and is thus an essential public health tool for controlling infectious disease outbreaks. For contact tracing to be effective, countries must have adequate capacity, including sufficient human resources, to test suspect cases in a timely manner.1 Technology can play a role in assisting Member States to implement contact tracing programs.

Member States have an obligation to develop public health [surveillance systems](https://www.who.int/publications-detail/surveillance-strategies-for-covid-19-human-infection)[[1]](#footnote-2) that capture data critical for COVID-19, while ensuring that such systems are transparent, are responsive to the concerns of communities, and do not impose unnecessary burdens.2 Failure to implement effective surveillance systems can hamper an effective public health and clinical response.3

Technology has the potential to improve surveillance through expanding the sources of appropriate and useful health data, improving the timeliness of data collection, and, when combined with machine learning and artificial intelligence, equipping public health agencies with information to make appropriate decisions. 4

A subset of digital technology for surveillance is proximity tracking (often conflated with ‘contact tracing’, although contact tracing is a broad public health discipline, and proximity tracking is a new technique for aiding contact tracing). Proximity tracking, which can be useful due to the availability of smartphones or other appropriate devices, relies on geographic positioning or local proximity sensing to identify the location or proximity of one person to another to enable tracing of potential exposures to infected individuals.

Digital proximity tracking cannot capture all the situations in which a user may acquire COVID-19, and it cannot replace traditional public health contact tracing, testing or outreach.In fact, digital proximity tracking applications can only be effective if there is also a corresponding public health infrastructure in place, and such digital proximity tracking applications, whether developed by the public or private sector, should be fully integrated into an existing health system and national pandemic response. This would need to include health services personnel, testing services and the manual contact tracing infrastructure. 5

Considering these limitations, digital proximity tracking could assist health authorities in notifying a person of an increased risk of exposure to another who has tested positive for COVID-19. Such notification of users that may have come in close contact with a COVID-19-positive individual could encourage a user to seek out testing (if such testing is available) or take precautions that limit transmission (e.g., self-isolation, physical distancing), even before an individual develops symptoms.6 Early public health response actions can make a significant difference between control and a resurgence of COVID-19. Furthermore, data generated by digital proximity tracking technologies could be useful for researchers to prepare for future outbreaks of COVID-19 and to assist general preparedness for future epidemics and pandemics.

Yet such uses of data could also threaten fundamental rights and liberties during and after the COVID-19 pandemic. Surveillance can quickly traverse the blurred line between disease surveillance and population surveillance. Thus, there is a need for laws, policies and oversight mechanisms that place strict limits on the use of digital proximity tracking technologies and research that uses data generated by such technologies.

Some private companies capture as many data as governments through their products, services, or platforms, may develop or are sharing their own digital proximity tracking applications, and in some cases are given the responsibility of collecting and analysing data. There is a broader concern that private companies may permanently integrate their products, services, and architecture within public health infrastructure. This could compromise a government’s full oversight and control of critical public health functions and services and facilitate the commercial exploitation of sensitive health data and services over the long term.

Member States can achieve public health objectives and protect fundamental rights such as privacy at the same time. Laws and human rights instruments do allow for use of data in the public interest, while also preventing unnecessary intrusions or commercial exploitation. Integrating ethical considerations into the design (programming) of a technology can ensure that its technical specifications preserve and promote certain values, such as transparency and privacy.

# The effectiveness of digital proximity tracking remains unknown

Digital proximity tracking technologies have been and are already being used in several countries in the COVID-19 response. Other governments, universities and companies are developing technologies at scale at a historically unprecedented speed, and digital technologies can be distributed widely after development within a largely unregulated environment. The effectiveness of such technologies depends mostly upon the underlying technology design and implementation approach and other factors, such as the level of uptake and the levels of confidence and trust that a population may vest in a chosen solution.

New technologies, such as digital proximity tracking, must be subject to rigorous review, especially to ascertain whether and when such technologies are effective. Measuring the effectiveness and impact of digital proximity tracking technologies is a prerequisite to building confidence in their reliability and trust in governmental or private entities that design, disseminate and manage these technologies. Assessing the effectiveness and impact of digital proximity tracking technologies can also assist the public and governments to determine if the trade-offs with privacy (or investments in other contact tracing strategies) is proportional to its public health impact. If such technologies do not prove effective against COVID-19, then the technology should be phased out. Currently, the effectiveness of digital proximity tracking remains unknown.

# Enabling environment for use of digital proximity tracking applications

While digital proximity tracking applications could play a useful role in supporting contact tracing for COVID‑19, these technologies are only one intervention within a wider system of policies, interventions, and investments. Governments and health systems should explain how this mix of policies, interventions and technologies would work together within an overall strategy.

Even if a digital proximity tracking application works in one country, these technologies may only be effective in other countries with sufficient technological infrastructure and safeguards to ensure ethical use. First, a country must already have widespread diffusion of smartphones or other appropriate devices and Internet access. Recent studies have estimated that a digital proximity tracking technology should be adopted by 60% to 75% of a country’s population to be maximally effective.7,8

Data protection and privacy laws should be in place, supported by additional legislation to provide a legal basis (and limits) for data processing, restrictions on data use, measures to establish oversight, and sunset clauses to dismantle use of the technology.9 There must also be a certain level of trust in government; otherwise individuals are unlikely to use digital proximity tracking applications, even if usage is fully voluntary. Finally, communities themselves should have awareness and understanding of how the tools work, in part to avoid discrimination or unfair targeting. Inclusive communication strategies that explain the purpose and use of the technologies should be designed so that they reach marginalized populations and vulnerable communities, while also ensuring users do not develop a false sense of security from use of such technologies.

Inequities could be exacerbated through use of these technologies.10 Digital proximity tracking applications only indirectly benefit those individuals without access to smartphones or other appropriate devices, and in general will only be beneficial to those who are already comfortable with the use of smartphones. Relying exclusively on digital proximity tracking will leave marginalized populations, especially the elderly, people living in poverty, and communities already suffering from stigmatization or exclusion, with even less access to essential services. Where appropriate, steps should be taken to improve voluntary access to such technologies in resource-limited settings, for example through lower mobile data costs or improved affordability and accessibility of low-cost devices.

# Suggested principles

To provide governments, public health institutions, non-State actors (non-governmental organisations, charities, foundations) and companies with guidance as to the ethical and appropriate use of digital surveillance technologies to address COVID-19, the following principles have been identified:

| **Principle** | **Explanatory Text** |
| --- | --- |
| **Time limitation** | All measures shall be temporary in nature and limited in scope. If governments and health systems expand monitoring and surveillance powers then such powers should be time bound, and only continue for as long as necessary to address the current pandemic. Measures should be fully withdrawn at the earliest moment after the pandemic has passed locally. There are legitimate concerns that digital proximity tracking will be unnecessary yet will remain in place. |
| **Testing and evaluation** | Digital proximity tracking technologies are novel and largely untested in many countries and settings. Every effort should be made to test the technologies prior to widespread use to ensure they function as intended, are technically robust, and have no security flaws. Governments and health systems should implement rigorous evaluation of the technology during the pandemic to continuously monitor that it is working effectively. The evaluations should be conducted by an independent agency or research body and should be published. |
| **Proportionality** | Collection and processing of personal data and health data shall be proportionate and provided by law. This means that collection of data for digital proximity tracking must be (a) justified by legitimate public health objectives; (b) suitable to achieve the intended goal; (c) necessary; and (d) reasonable and proportionate to the aims pursued. The latter requirement entails assessing the value of colliding rights vis-à-vis the impact intensity of surveillance activities on each person. The least intrusive (privacy-preserving) measures should always be preferred for an application’s design, including avoiding the use of physical location (geographic position) tracking for digital proximity tracking. |
| **Data minimization** | Data collection, retention and processing shall be limited to the minimum necessary amount of data that is needed to achieve the public health objective. Thus, data collection should not require the identity or location data of a user, or a time stamp of a proximity event (though the date of a proximity event may be useful). Data collected, retained and aggregated must be limited in scope. |
| **Use restriction** | The sale and use of data for commercial purposes or advertising activities should be strictly prohibited. Recognizing that governments may have existing data protection laws and frameworks already in place, the sharing of data with government departments, agencies or third parties that are not involved in the public health response should be prohibited. The sharing of data with law enforcement or immigration departments or agencies should also be prohibited. |
| **Voluntariness** | An individual’s decision to download and use an application that contributes to public health surveillance or digital proximity tracking should be voluntary and informed. Governments should not mandate use of such an application. Additional incentives or inducements by either a government or private parties should not be bestowed on those individuals who download and use such an application. No individual should be denied services or benefits from either a government or private parties for refusing to use an application, including the right to use health services, the receipt of economic aid in the context of a pandemic or thereafter, or the use of a phone that is provided by a company for work-related purposes. An individual should be free to turn off the application at any time and should be free to delete the application at any time without any consequences, as well as to delete any data that may have been collected and stored, including retroactively redacting blocks of time that the user does not wish to upload. |
| **Transparency and explainability** | Data collection and processing shall be transparent, and individuals shall be provided with concise and reader-friendly information in clear and unambiguous language regarding the purpose of collection, the types of data collected, how data will be stored and shared, and how long data shall be retained. There should be full transparency about how the applications and application programming interface (APIs) operate, and publication of open source and open access codes. Individuals should also be provided with meaningful information about the existence of automated decision-making and how risk predictions are made, including how the algorithmic model was developed and the data used to train the model. Furthermore, there should be information about the model’s utility and insights as to the types of errors that such a model may make. |
| **Privacy-preserving data storage** | There are differing views as to whether data storage should be decentralized or centralized, including which approach to data storage is more effective and secure. Both approaches may preserve privacy but both approaches also have vulnerabilities that must be addressed, including the security of data that are collected and stored. There is an emerging consensus, including opinions issued recently by several data protection authorities, that decentralized approaches enhance privacy, since they provide users with greater control (including the exercise of consent or withdrawal of consent) over the quantum of information that a user may share with health authorities. The collection and use of such data by health authorities can therefore be limited to what is strictly necessary for the operation of a digital proximity tracking system. Whichever approach is selected, governments and third parties should ensure it is in conformity with expectations of privacy and the principles included in this guidance. |
| **Security** | Every effort should be made to ensure high security, including encryption, of any personal data or health data collected and of any devices, applications, servers, networks, or services involved in collection, transmission, processing, and storage. Applications should be subject to third-party audits and penetration testing, and developers should publish full details about their security protocols. |
| **Limited retention** | Data retention shall be limited to the period of the pandemic response, except for the purposes of research or epidemic planning, subject to appropriate regulation, oversight, and informed consent, where required. Data utilized for research or epidemic planning should be aggregated and anonymized where possible. Where aggregation of data is not possible for research purposes, such exceptions should be justified, and all such data should still be anonymized. Data collected for public health purposes related to COVID-19 shall be deleted following the pandemic. To the extent technically feasible, any technologic system created should be dismantled at the end of the pandemic. |
| **Infection reporting** | The reporting into a digital proximity tracking application that a user has tested positive for COVID-19 could be done through several channels. In any scenario, notification of the application should require the consent of the individual. In one scenario, a user of a digital proximity tracking application could self-report an infection to the application. A health system must determine if such self-notification must be confirmed by a health professional. Alternatively, upon a patient being confirmed as positive for COVID-19, a medical professional could notify the digital proximity tracking application (with the individual’s consent). |
| **Notification** | Notification of individuals who may have been in contact with a person infected with COVID-19 could, for example, be delivered directly by an application to close contacts. The notification of other users must preserve the privacy of the infected individual. Users who receive a notification through their device should receive information on steps that they should take. Such notification should be provided in clear, accessible language and explain the options that users have (including any consequences attached to these options). Such notification should be accessible to all people – information should be provided in several languages and be accessible to people with disabilities. Users should be able to consent as to whether they wish to have the health authorities contact them for follow-up (for example, testing), including disclosure of their contact information to the health authorities. A user who has been notified by an application should not be penalized, punished, or denied medical services or economic benefits for failing to follow instructions provided by the application. |
| **Tracking of COVID-19-positive cases** | After an individual who uses a digital proximity tracking application has tested positive for COVID-19, the application should not be used to track that individual’s movements during his or her period of infection and recovery, including whom that individual may encounter thereafter. |
| **Accuracy** | Algorithmic models used to process data and assess risk of transmission must bereliable, verified and validated. Such applications should be open to testing by third parties and risk models should be developed with epidemiologists to establish parameters for duration and proximity before a contact is recorded and should be adjusted and improved over time. Data quality should be assessed for biases to avoid any adverse effects, including giving rise to unlawful and arbitrary discrimination. |
| **Accountability** | Any response must incorporate accountability protections and safeguards against abuse. Individuals must be given the opportunity to know about and challenge any COVID-19-related measures to collect, aggregate, retain and use data. Individuals subjected to unwarranted surveillance must have access to effective remedies and mechanisms of contestation. |
| **Independent oversight** | There should be independent oversight, including ethics and human rights aspects, of both public agencies and businesses that develop, operate, or use information obtained from digital proximity tracking applications. Such oversight could include the establishment of an independent oversight body. The existence of agreements between government and business, and information necessary to assess their impact on privacy and human rights, must be publicly disclosed, along with sunset clauses and oversight. Such oversight must ensure that any use of digital proximity tracking applications by governments is firewalled from other government functions and, in the case of companies, from other business and commercial interests. An oversight body must also have access to all information necessary to ascertain that digital proximity tracking measures are necessary and proportionate to their impact and effectiveness. An oversight body should also monitor the collection and use of data to ensure they are consistent with laws and regulations and prevent abuse or exploitation of vulnerable and marginalized communities. Finally, an independent oversight body should remain in place after the end of the pandemic to ensure that digital proximity tracking technologies are fully dismantled. The effectiveness of any independent oversight body depends in part on the codification and enforcement of ethical standards and human rights principles and conventions by governments, and respect for such principles and standards by governments and businesses. |
| **Civil society and public engagement** | COVID-19-related responses that include data collection efforts should include free, active, and meaningful participation of relevant stakeholders, such as experts from the public health sector, civil society organizations, and the most marginalized groups. This participatory approach is not only mandated from an ethics perspective – it will also enhance buy-in, voluntary participation and compliance. Furthermore, civil society can play a crucial role in holding governments and companies accountable for the deployment and operation of digital proximity tracking technologies. |

References

1. Contact tracing in the context of COVID-19: interim guidance. Geneva; World Health Organization; 2020 (<https://www.who.int/publications-detail/contact-tracing-in-the-context-of-covid-19>, accessed 21 May 2020)
2. Surveillance strategies for COVID-19 human infection: interim guidance. Geneva; World Health Organization; 2020 (<https://www.who.int/publications-detail/surveillance-strategies-for-covid-19-human-infection> , accessed 21 May 2020)
3. WHO guidelines on ethical issues in public health surveillance. Geneva; World Health Organization; 2017 (<https://apps.who.int/iris/bitstream/handle/10665/255721/9789241512657-eng.pdf?sequence=1>, accessed 7 May 2020)
4. Wong, Zoie & Zhou, Jiaqi & Zhang, Qingpeng. (2018). Artificial Intelligence for infectious disease Big Data Analytics. Infection, Disease & Health. 24. 10.1016/j.idh.2018.10.002.
5. American Civil Liberties Union. Principles for technology-assisted contact-tracing. ACLU White Paper; 2020 (<https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing>, accessed 7 May 2020).
6. Parker MJ, Fraser C, Abeler-Dörner L*, et al. (2020).* Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics*. (<https://jme.bmj.com/content/early/2020/05/05/medethics-2020-106314>, accessed 10 May 2020)
7. Effective configuration of a Digital Contact Tracing App: A report to NHSX; 2020 (<https://github.com/BDI-pathogens/covid-19_instant_tracing/>, accessed 21 May 2020)
8. Ada Lovelace Institute. Exit through the app store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis. Ada Lovelace Institute; 2020 (<https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf>, accessed 7 May 2020)
9. Council of Europe. Joint statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108, and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. Strasbourg: 30 March 2020 (<https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter>, accessed 7 May 2020).
10. The Age of Digital Interdependence: Report of UN Secretary-General’s High-level Panel on Digital Cooperation. UN Secretary General’s High Level Panel on Digital Cooperation; 2019 (<https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf>, accessed 21 May 2020)

# Bibliography

Amnesty International and others. Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights. 2 April 2020 (<https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf>, accessed 7 May 2020).

Crocker A, Opsahl K, Cyphers B. The challenge of proximity apps for COVID-19 contact tracing. Electronic Frontier Foundation; 2020 (<https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing>, accessed 7 May 2020).

DP-3T. Decentralized privacy-preserving proximity tracing. DP-3T; 2020 (<https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf>, accessed 7 May 2020).

European Commission. Communication from the Commission: guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection. Brussels: European Commission; 2020 (<https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf>, accessed 7 May 2020).

European Data Protection Board. Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020 (<https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>, accessed 7 May 2020).

NEK. Contact tracing als Instrument der Pandemiebekämpfung: Zentrale Gesichtspunkte aus der Perspektive der Ethik [Contact tracing as an instrument to fight pandemics: central aspects from the perspective of ethics]. Opinion No. 33, 2020. Berne: Swiss National Ethics Committee in the Field of Human Medicine (NEK); 2020 (<https://www.nek-cne.admin.ch/inhalte/Themen/Stellungnahmen/NEK-stellungnahme-Contact_Tracing.pdf>, accessed 7 May 2020).

United Nations Development Group. Data privacy, ethics and protection guidance note on big data for achievement of the 2030 Agenda (<https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf>, accessed 7 May 2020).

Acknowledgements

This document was developed in consultation with:

Najeeb Al-Shorbaji (eHealth Development Association, Amman, Jordan); Zeke Emanuel (University of Pennsylvania, Philadelphia, US); Partha Majumder (National Institute of Biomedical Genomics, Bangalore, India); Timo Minssen (University of Copenhagen, Copenhagen, Denmark); Michael Parker (University of Oxford, Oxford, UK); María Paz Canales (Derechos Digitales, Santiago de Chile, Chile); Rasha Abdul Rahim (Amnesty International, London, UK); Jerome Singh (University of KwaZulu-Natal, Durban, South Africa); Maxwell Smith (Western University, London, Canada); Beatriz Thome (Universidade Federal de Sao Paulo, Sao Paulo, Brazil); Tze-Yun Leong (National University of Singapore, Singapore); Ross Upshur (University of Toronto, Toronto, Canada); Jeroen Van den Hoven (Delft University of Technology, Delft, The Netherlands); Effy Vayena (Chair of the Working Group, ETH Zurich, Zurich, Switzerland); Yi Zeng (Chinese Academy of Sciences, Beijing, China).

From World Health Organization:

Patrick Anthony Drury, Clayton Hamilton, Katherine Littler, Rohit Malpani, Boris Pavlin, Sameer Pujari, Andreas Reis.

WHO continues to monitor the situation closely for any changes that may affect this interim guidance. Should any factors change, WHO will issue a further update. Otherwise, this interim guidance document will expire 2 years after the date of publication

© World Health Organization 2020. Some rights reserved. This work is available under the [CC BY-NC-SA 3.0 IGO](https://creativecommons.org/licenses/by-nc-sa/3.0/igo) licence.

WHO reference number: WHO/2019-nCoV/Ethics\_Contact\_tracing\_apps/2020.1

1. The International Health Regulations (2005) define surveillance as “the systematic ongoing collection, collation and analysis of data for public health purposes and the timely dissemination of public health information for assessment and public health response as necessary”. [↑](#footnote-ref-2)